COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

PARECER/2020/80

I. Pedido

1. Em 22 de novembro de 2019, por despacho do Secretário de Estado Adjunto e da Administração Interna, foi solicitado parecer à Comissão Nacional de Proteção de Dados (CNPD) sobre o pedido de autorização de alargamento do sistema de videovigilância na cidade de Amadora, submetido pela Polícia de Segurança Pública (PSP).

Na sequência do pedido, por parte da CNPD, de informação complementar, datado de 16 de janeiro de 2020, foram remetidos, em 12 de junho de 2020, esclarecimentos suplementares, bem como a avaliação de impacto sobre a proteção de dados relativa àquele sistema.

A CNPD aprecia o pedido nos termos e para os efeitos da Lei n.º 1/2005, de 10 de janeiro, alterada e republicada pela Lei n.º 9/2012, de 23 de fevereiro, que regula a utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, para captação e gravação de imagem e som e seu posterior tratamento.

II. Apreciação

1. Objeto do parecer a emitir nos termos do artigo 3.º da Lei n.º 1/2005, de 10 de janeiro

Nos termos do n.º 2 do artigo 3.º da Lei n.º 1/2005, de 10 de janeiro, na redação dada pela Lei n.º 9/2012, de 23 de fevereiro (doravante, Lei n.º 1/2005), o parecer da CNPD restringe-se à pronúncia sobre a conformidade do pedido com as regras referentes à segurança do tratamento dos dados recolhidos, bem como acerca das medidas especiais de segurança a implementar adequadas a garantir os controlos de entrada nas instalações, dos suportes de dados, da inserção, da utilização, de acesso, da transmissão, da introdução e do transporte e, bem assim, à verificação do cumprimento do dever de informação e perante quem os direitos de acesso e retificação podem ser exercidos.

De acordo com o disposto no mesmo preceito legal e nos n.ºs 4, 6 e 7 do artigo 7.º daquela lei, é também objeto do parecer da CNPD o respeito pela proibição de instalação de câmaras fixas em áreas que, apesar de situadas em locais públicos, sejam, pela sua natureza, destinadas a ser utilizadas em resguardo ou a utilização de câmaras de vídeo quando a captação de imagens e de sons abranja interior de casa ou edifício habitado ou sua

dependência, ou quando essa captação afete, de forma direta e imediata, a intimidade das pessoas, ou resulte na gravação de conversas de natureza privada.

Deve ainda a CNPD verificar se estão assegurados, a todas as pessoas que figurem em gravações obtidas de acordo com a presente lei, os direitos de acesso e eliminação, com as exceções previstas na lei.

Nos termos do n.º 7 do artigo 3.º do mesmo diploma legal, pode também a CNPD formular recomendações tendo em vista assegurar as finalidades previstas na lei, sujeitando a emissão de parecer totalmente positivo à verificação da completude do cumprimento das suas recomendações.

2. Os tratamentos de dados pessoais não legitimados pela Lei n.º 1/2005

Não obstante não caber, nos termos das competências legais definidas na Lei n.º 1/2005, à CNPD pronunciar-se sobre a proporcionalidade da utilização de sistemas de videovigilância em locais públicos de utilização comum para a finalidade de proteção de pessoas e bens, essa competência já existe quando em causa estejam câmaras instaladas em áreas que sejam, pela sua natureza, destinadas a ser utilizadas em resguardo ou a captação de imagens ou som abranja interior de casa ou edifício habitado ou sua dependência ou afete, de forma direta e imediata, a intimidade das pessoas, ou resulte na gravação de conversas de natureza privada (cf. n.ºs 4, 6 e 7 do artigo 7.º da Lei n.º 1/2005).

Ora, o alargamento do sistema de videovigilância na cidade da Amadora[1] implica um tratamento de dados pessoais que, pelo seu âmbito e extensão, parece afetar significativamente a vida privada das pessoas que circulem ou se encontrem naquela cidade.

---

[1] Pretende-se, conforme consta do pedido de autorização de alargamento do sistema de videovigilância, a cobertura total ou parcial de um extenso leque de artérias da cidade de Amadora, "*tendo em conta que são os locais de maior índice de criminalidade na área Central do Concelho da Amadora – concretamente os* [sediados] *nas Freguesias Mina de Água, Encosta do Sol, Venteira, Falagueira-Venda, Águas Livres e Alfragide*", utilizando para o efeito um total de 141 câmaras. Para além da extensão do tratamento de dados pessoais, deve aqui considerar-se ainda que tais câmaras têm capacidade de rotação e ampliação da imagem, o que significa a capacidade de captar, em todas as direções e com grande acuidade, imagens de pessoas e veículos.

Não se pretende aqui discutir a necessidade dessa extensão, mas antes recentrar a análise do pedido na adequação do tratamento de dados pessoais para a finalidade legalmente prevista invocada pelo requerente.

Sendo declarado no pedido que a finalidade do tratamento é a de garantir a proteção da segurança de pessoas e bens, públicos e privados, assim como assegurar a prevenção de crimes em que exista razoável risco da sua ocorrência, finalidade essa que tem enquadramento legal (cf. alínea *c)* do n.º 1 do artigo 2.º da Lei n.º 1/2005), cumpre aqui assinalar, desde logo, que se continua a invocar como factos justificativos deste tipo de pedidos o combate às "*incivilidades*" ou a prevenção e dissuasão de "*condutas anti-sociais*", bem como a necessidade do sistema para criar "*sentimento de segurança*". Sucede que estes fundamentos estão claramente fora do âmbito de aplicação da Lei n.º 1/2005, máxime da alínea *c)* do n.º 1 do artigo 2.º. Na verdade, esta específica disposição legal apenas legitima a utilização de sistemas de videovigilância como apoio na função de prevenção ou repressão de condutas que ponham efetivamente em causa a segurança de pessoas e bens – e por essa razão se especifica a prevenção de condutas ilícitas qualificadas como crime – , por só essas assumirem relevância suficiente para justificar a restrição de direitos fundamentais dos cidadãos, como o direito à reserva ou ao respeito pela vida privada e o direito à liberdade. Incivilidades ou outras condutas que, ainda que ilícitas, se apresentam em tensão com a mera ordenação social, merecem, quando muito, um juízo de censurabilidade menor pelo ordenamento jurídico e, por isso, não justificam a legitimação da restrição de direitos, liberdades e garantias por via deste tipo de sistemas de informação.

Mais preocupante é a referência, repetida a propósito das câmaras n.º 62 a 139, de que com as mesmas se pretende a "*monitorização da circulação de pessoas, viaturas e bens*" (cf. anexo K – Fichas individuais das câmaras). A pretensão de utilizar um sistema de videovigilância, com o âmbito e extensão do aqui considerado, para monitorizar a circulação de pessoas e viaturas vai muito para além da finalidade legalmente definida, não tendo, na verdade, qualquer enquadramento legal.

A segurança das pessoas e dos bens e a prevenção criminal não fundamentam diretamente o acompanhamento e rastreamento permanente das pessoas (e viaturas) no espaço público, precisamente porque esta é uma finalidade diferente daquela. Poderá admitir-se que, por via da prossecução desta, se consiga ainda contribuir para a realização da finalidade prevista na alínea *c)* do n.º 1 do artigo 2.º da Lei n.º 1/2005, mas os objetivos são bem distintos e essa diferença não é apenas de grau de intensidade. A monitorização permanente das

pessoas, viaturas e dos bens nas vias públicas da cidade de Amadora garante o acompanhamento e o controlo das pessoas (quanto à deslocação, às interações humanas no espaço público e demais comportamentos), ultrapassando, como se referiu, a finalidade de prevenção e repressão criminais.

E este objetivo é ainda reforçado pela referência no pedido da PSP à utilização de tecnologias de Inteligência Artificial e de sistema biométrico de reconhecimento facial, os quais, como melhor se explicará em seguida, são suscetíveis de potenciar esse controlo.

Ora, não sendo a CNPD insensível, como ninguém seguramente o é na sociedade portuguesa, à necessidade de as pessoas se sentirem seguras para gozarem a sua liberdade e as outras dimensões fundamentais essenciais ao desenvolvimento da sua personalidade, necessidade essa invocada na fundamentação que acompanha o pedido – ainda que a referida fundamentação seja apresentada num estilo sensacionalista, que prejudica a objetividade que um documento oficial reclamaria –, não se pode esquecer que a lei nacional fixa pressupostos claros para a utilização dos sistemas de videovigilância, desde logo as finalidades admissíveis, e que, portanto, fora desses pressupostos nenhum organismo público pode recorrer a estes meios auxiliares para a sua atividade.

Recorda-se que, como de resto se refere na fundamentação do pedido, o direito fundamental à reserva da vida privada corresponde, no contexto do espaço público, a um direito ao anonimato. Aliás, foi com o sentido de *right to be let alone* que o direito à privacidade foi primeiramente afirmado, sendo inegável que o artigo 26.º da Constituição da República Portuguesa (CRP) e o artigo 7.º da Carta dos Direitos Fundamentais da União Europeia (Carta) também o protegem nessa dimensão. Para sua salvaguarda, bem como para salvaguarda do direito fundamental à liberdade, em especial de circulação no território português e no espaço público (cf. artigo 27.º da CRP e, no território dos Estados-Membros da União Europeia, artigo 6.º da Carta), a lei portuguesa definiu o conjunto de fins de interesse público que podem justificar a compressão destes direitos fundamentais e que se prendem, ora com o direito fundamental à segurança e o interesse público da segurança, ora com o direito à propriedade. Mas o regime legal, como não podia deixar de ser, procura conciliar os diferentes direitos e interesses que considerou pertinentes de modo que se previna a afetação do conteúdo essencial dos direitos fundamentais dos cidadãos (donde os limites definidos nos n.ºs 4, 6 e 7 do artigo 7.º da Lei n.º 1/2005) – cf. artigo 18.º da CRP e artigo 52.º da Carta. Este equilíbrio deve ser concretizado precisamente no ato autorizativo

do Ministro da Administração Interna (ou do órgão delegado), sempre salvaguardando o conteúdo essencial dos direitos fundamentais à reserva da vida privada e da liberdade.

É certo que a liberdade depende também, para o seu gozo pleno, de segurança – como, aliás, é sublinhado por várias vezes na fundamentação do pedido, onde se pode ler que "*uma parte (muito significativa) da população, tende a constranger os seus movimentos em função do nível de segurança percepcionado, o que – isso sim- representa uma genuína e realística perda de Liberdade*". Mas não é menos certo que, se a garantia da segurança – fundada na própria liberdade – implicar uma restrição da liberdade em termos tais que esta é afetada no seu núcleo essencial, então cessa a razão de ser dessa restrição e a razão de ser da efetivação da segurança.

Ora, a monitorização da circulação de pessoas, viaturas e bens nas diferentes vias públicas da cidade da Amadora implica um controlo da deslocação e de comportamentos das pessoas insuportável em termos de afetação, não apenas da privacidade, mas também da sua liberdade, desde logo por força da possibilidade de (muito fácil) rastreamento das deslocações e comportamentos dos cidadãos. Importa, pois, sublinhar que o objetivo declarado de *monitorização da circulação de pessoas, viaturas e bens* não tem enquadramento na Lei n.º 1/2005, nem é constitucionalmente admissível, por implicar a restrição do conteúdo essencial dos direitos à reserva da vida privada e da liberdade.

Na verdade, a restrição destes direitos fundamentais com esta intensidade supõe a prévia suspensão do seu exercício, como aliás sucedeu com o decretamento do estado de emergência durante um período inicial da pandemia. Recorda-se que a suspensão do exercício da liberdade de deslocação tornou lícita a monitorização das deslocações dos cidadãos pelas forças e serviços de segurança para garantir a efetivação do confinamento social imposto, alguns dos quais implicaram, com fundamento na sua necessidade, a restrição do direito fundamental ao respeito pela vida privada. Só nesse quadro, definido no artigo 19.º da CRP, é que é suportável uma restrição que afete o conteúdo essencial dos direitos fundamentais e, mesmo aí, com caráter temporário e na estrita medida do necessário.

3. Videovigilância em locais públicos de utilização comum na cidade da Amadora para a finalidade de proteção de pessoas e bens e prevenção de crimes

Pretende-se instalar na cidade da Amadora 38 câmaras, a acrescer às 103 já existentes, das quais 5 são reposicionadas, num total de 141 câmaras.

As novas câmaras, que são do modelo *BOSCH MIC IP starlight 7100*, estão capacitadas com funcionalidades de *vídeo analytics*. Destaca-se, a título exemplificativo, que a função *Intelligent Tracking*, de que as mesmas estão dotadas, permite que o sistema aplique zoom de forma automática e acompanhe continuamente o movimento do "objeto" (*target*) selecionado pelo operador – o objeto pode corresponder a uma pessoa ou uma viatura. As câmaras da gama 7000i dispõem ainda da função *Camera Trainer*: um mecanismo de *Machine Learning* que permite selecionar um "objeto" para reconhecimento pelo sistema em futuras captações de imagem.

3.1. Utilização de tecnologias de Inteligência Artificial e reconhecimento facial

Começa-se por analisar, pela sua relevância para a esfera jurídica dos cidadãos, a seguinte referência no pedido de fundamentação: "*As câmaras têm capacidade de iluminação, resolução e ampliação que proporciona qualidade de visualização, tanto no período noturno como diurno, garantindo: reconhecimento de indivíduos, nos termos do Regulamento CE n.º 2252/2004, do Conselho, de 13 de dezembro; deteção de faces, deteção de movimento e deteção de objetos abandonados*".

Como a CNPD já teve oportunidade de sublinhar noutra sede, a utilização de Inteligência Artificial (IA) associada aos sistemas de videovigilância em espaço público pode revelar-se útil e portanto adequada, em determinadas condições, na prossecução da finalidade proteção da segurança das pessoas e bens e prevenção da prática de crimes em locais em que exista razoável risco da sua ocorrência – a finalidade que, nos termos legais, pode ser visada com a utilização deste sistema de videovigilância.

Mas, mesmo para a prossecução da finalidade de proteção da segurança de pessoas e bens em relação a condutas criminalizadas – onde a IA se poderá revelar adequada –, a utilização desta tecnologia, em especial de *soft recognition*, porque permite o rastreamento da deslocação e dos comportamentos das pessoas, carece de uma específica demonstração da necessidade da sua utilização, o que no caso concreto não sucede. De facto, em ponto

nenhum da referida fundamentação se explica a necessidade dessa específica tecnologia e funcionalidade: nem no anexo B, onde se descrevem as características técnicas do sistema, nem nos fundamentos apresentados no Anexo D; nem ainda nos esclarecimentos entretanto prestados e na avaliação de impacto sobre a proteção de dados, na qual está omissa a análise desta tecnologia.

Acresce que a ausência de descrição dos algoritmos envolvidos na comparação e deteção de padrões, a falta de especificação de quem é responsável pela definição desses padrões e ainda a omissão de especificação dos critérios envolvidos nesses padrões (*v.g.,* que padrões visuais o sistema usa para diferenciar um homem de uma mulher; quais são as taxas de tolerância configuradas para falsos positivos/negativos), tornam impossível a avaliação da sua adequação e necessidade para a finalidade de repressão criminal.

Repare-se que a utilização dos sistemas de videovigilância com soluções tecnológicas de IA, em particular de *soft recognition,* é suscetível de gerar um *risco elevado para os direitos, liberdades e garantias das pessoas*, nomeadamente os direitos ao respeito pela vida privada, à liberdade e à igualdade, uma vez que o risco de rastreabilidade de comportamentos e hábitos, bem como a seleção de características físicas e biométricas para a analítica de vídeo, pode gerar o condicionamento da liberdade de ação e controlos discriminatórios a partir de determinados perfis. Nessa medida, a avaliação de impacto realizada em cumprimento do disposto no artigo 29.º da Lei n.º 59/2019, de 8 de agosto[2], tinha, obrigatoriamente, de incidir sobre a utilização desta tecnologia neste contexto.

E não pode, de todo, pretender concluir-se sem mais pela adequação e necessidade da utilização de um específico instrumento tecnológico (que é especialmente reconhecido pela sua dimensão impactante sobre os direitos e liberdades das pessoas) apenas por apelo à segurança, simplificando-se o raciocínio com a conclusão da preponderância deste valor sobre os direitos e liberdades individuais. Na realidade, a busca inteligente de imagens em arquivo e, especificamente, a deteção de objetos abandonados assenta em algoritmos programados para responder a estímulos e movimentos específicos, mas, como se sublinhou, em ponto algum dos elementos que integram e complementam o pedido se esclarece qual o algoritmo a utilizar, de que pressupostos o mesmo partirá e quais as

[2] Lei que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

respostas (*outputs)* que se pretende atingir. Sem essa informação, não se consegue perceber se os resultados da sua utilização, e com base nos quais a PSP vai tomar decisões sobre os cidadãos visados, são ou não discriminatórios e, portanto, inadmissíveis à luz da Constituição da República Portuguesa.

Assim, nos termos em que é apresentada a utilização desta tecnologia, o parecer da CNPD, quanto à sua utilização, só pode ser negativo.

Mas o presente pedido de alargamento do sistema de videovigilância vai mais longe. Nele se prevê a utilização de *reconhecimento facial, quando se refere o "reconhecimento de indivíduo, nos termos do Regulamento CE n.º 2252/2004, do Conselho de 13 de dezembro".* É certo que este diploma vem referido na alínea *b)* do n.º 1 do Anexo à Portaria n.º 372/2012, de 16 de novembro. Simplesmente, o diploma europeu citado estabelece normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros, procurando assegurar a harmonização dos dispositivos de segurança, incluindo os identificadores biométricos. Ora, tendo em conta o objeto e âmbito deste diploma da União Europeia, pensado para garantir a identificação de pessoas na entrada e saída do espaço Schengen e da União, o mesmo não serve para legitimar o reconhecimento facial dentro de uma cidade. Vejamos.

Sendo certo que o tratamento de dados biométricos destinados a identificar uma pessoa singular de forma inequívoca só pode ser efetuado nas circunstâncias especificadas no n.º 1 do artigo 6.º da Lei n.º 59/2018, de 8 de agosto, é por demais evidente a ausência de fundamento de licitude da realização do tratamento de dados pessoais por via de reconhecimento facial em sistema de videovigilância num espaço público como o da cidade da Amadora. Na verdade, o referido artigo só considera legítimo tal tratamento se o mesmo *for estritamente necessário, se estiver sujeito a garantias adequadas de proteção dos direitos e liberdades do titular dos dados e se: for autorizado por lei, se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular ou se estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados.*

Além da necessidade da sua utilização não estar demonstrada em ponto algum da fundamentação, nem aí se fixarem garantias adequadas de proteção dos direitos e liberdades tendo em conta esta específica tecnologia, nem tão-pouco a mesma ser focada

na avaliação de impacto sobre a proteção de dados apresentada, não se encontra verificado qualquer dos fundamentos de licitude previstos naquele artigo.

Com efeito, não existe lei a prever a sua utilização em associação a um sistema de videovigilância em espaço público; tão-pouco pode a utilização sistemática e generalizada do sistema de videovigilância com reconhecimento facial assentar no fundamento de proteção de interesses vitais do próprio titular dos dados ou de terceiros, porque não se pode afirmar que haja perigo de vida das pessoas naquele concelho de modo permanente ou sistemático. Finalmente, o terceiro fundamento – dados manifestamente tornados públicos pelo respetivo titular – não tem, evidentemente, aplicação aos dados biométricos, uma vez que a base de dados a partir da qual se faria o reconhecimento facial resulta da recolha de dados biométricos efetuada por imposição legal[3], não podendo ser por isso imputado a uma suposta vontade do titular o tratamento ulterior dos mesmos.

Assim, não se alcança como pode pretender-se associar a utilização de tecnologia de reconhecimento facial ao sistema de videovigilância na cidade da Amadora.

Assinale-se, ainda assim, que o reconhecimento facial generalizado numa cidade sempre constituirá uma medida que exige uma fundamentação particularmente reforçada, considerando o risco de controlo dos cidadãos que a sua utilização pelas forças de segurança necessariamente implica. Não há apenas afetação da liberdade individual de circulação e de comportamento. Há também um risco elevado de perturbação da sociedade democrática, como em outros pontos do mundo tem vindo a ser demonstrado. Pelo que o legislador nacional só pode avançar para a legitimação de uma tal solução em circunstâncias muito especiais, espacial e temporalmente delimitadas e sob condições e critérios de utilização precisos e claramente definidos. É essencial assegurar, quanto a esse tipo de tecnologia, a previsibilidade para os cidadãos das condições e consequências dos tratamentos de dados desta natureza e impacto. Deve, em especial, ponderar-se quais os tipos de crimes que poderão justificar a sua utilização e em que medida se revela adequada a prevenir ou reprimir esses ilícitos e em que exatas áreas territoriais de uma cidade essa adequação e necessidade se manifesta.

Tendo a CNPD sublinhado a obrigação de realização da avaliação de impacto sobre a proteção de dados imposta pelo artigo 29.º da Lei n.º 59/2019, de 8 de agosto, é

[3] Seja a base de dados de identificação civil, seja as bases de dados criadas no âmbito da investigação criminal.

incompreensível que a avaliação entretanto apresentada seja omissa quanto a este aspeto do sistema.

Considerando que há um conjunto de dados pessoais que estão sujeitos a um regime especialmente reforçado de proteção – os previstos no n.º 1 do artigo 6.º da Lei n.º 59/2019, de 8 de agosto – e que o n.º 2 do mesmo artigo proíbe a criação de perfis que conduzam à discriminação de pessoas singulares com base nesses dados, a CNPD entende que a utilização deste tipo de sistema biométrico tem de ser, no mínimo, precedida de um conjunto de regras precisas para os utilizadores da mesma, de modo a limitar o risco de discriminação e de violação do artigo 6.º da referida lei. Sem isso só pode concluir pela sua não admissibilidade.

3.2. Outros aspetos do tratamento de dados pessoais

Considerando agora outras características técnicas do sistema de videovigilância, importa destacar os seguintes aspetos que suscitam reservas à CNPD.

3.2.1. Declara-se no ponto 7 do Anexo D que acompanha o pedido, que "*as câmaras de vídeo garantem a criação de máscaras de privacidade, de modo a omitir a imagem das áreas privadas (portas, janelas, varandas, terraços de edifícios de casas de habitação, quintais, etc.)*", tendo em vista o cumprimento dos limites fixados nos n.ºs 6 e 7 do artigo 7.º da Lei n.º 1/2015. Todavia, nas informações suplementares, esclarece-se que "[*e]xiste a possibilidade de desativação das máscaras pelos operadores, mas apenas nas situações estritamente necessárias de índole criminal de maior relevo, mediante autorização do Comando da Divisão, ficando esse procedimento devidamente registado em relatório.*"

Para além de parecer haver contradição entre o afirmado e a declaração subsequente de que as "*máscaras apenas podem ser criadas, alteradas e apagadas diretamente na câmara, pelo que nenhum operador tem acesso a esta funcionalidade. Apenas disponível para o administrador de sistema*", a CNPD considera que esta possibilidade viola o disposto nos n.ºs 4, 6 e 7 do artigo 7.º da Lei n.º 1/2005. Com efeito, se a lei impõe como limite ao tratamento a existência de soluções que previnam a afetação da privacidade dos cidadãos quando os mesmos se encontrem nas suas casas ou outras dependências, bem como em locais públicos destinados a utilização com resguardo, o sistema de videovigilância não pode permitir o afastamento deste limite, sob pena de uma eventual autorização a ser emitida neste procedimento violar o artigo 7.º da Lei n.º 1/2015.

De todo o modo, sempre se destaca que, ainda que tal fosse admissível, a solução de segurança adotada seria manifestamente insuficiente para garantir a integridade da configuração do sistema, uma vez que o (re)armazenamento da *password* após a sua utilização não garante a confidencialidade da mesma. Impor-se-ia, por isso, que cada utilização de palavra-passe fosse seguida da geração de uma nova palavra-passe e consequente armazenamento em local seguro.

Além disso, para efeito de auditabilidade do sistema, não seria nunca suficiente o registo do procedimento em relatório. Seria imprescindível garantir que o próprio sistema produzisse um *log* dessa operação com identificação do utilizador, da data e hora do evento, e das máscaras desativadas.

Assim, a CNPD entende não ser admissível a desativação das máscaras destinadas a garantir a privacidade, sob pena de violação do disposto nos n.ºs 4, 6 e 7 da Lei n.º 1/2005.

3.2.2. No que diz respeito às garantias de auditabilidade do sistema, mesmo após a prestação de informações suplementares, apenas se esclareceu existirem *logs*, sem que tivesse sido confirmado que os registos são realizados de forma encriptada, assinados digitalmente e com *time stamp.* Nessa medida, o sistema não parece cumprir o disposto no n.º 3 do artigo 4.º da Portaria n.º 372/2012, de 16 de novembro, nem o disposto no n.º 6 do artigo 27.º da Lei n.º 59/2019, de 8 de agosto, devendo, por isso, assegurar-se o respeito por esta exigência.

Quanto ao período de conservação dos *logs*, este não pode ficar limitado pela capacidade da base de dados. Assim, estando determinado um período de conservação de dois anos, na eventualidade de se ultrapassar a capacidade máxima indicada (4GB), deve ser garantida a exportação da informação para outro ficheiro.

3.2.3. Relativamente aos postos de trabalho (*desktop*) que interligam ao *videowall*, tem de ser desativada a função de captura de ecrã, de modo a obedecer ao dever legal de assegurar, desde o momento da conceção do sistema, as medidas necessárias para garantir o respeito pelos princípios da proteção de dados, em especial os previstos nas alíneas *c)* e *f)* do n.º 2 do artigo 4.º da Lei n.º 59/2019, de 8 de agosto.

Do mesmo modo e com os mesmos fundamentos legais, os periféricos existentes na Central de monitorização das imagens têm de estar desativados, reforçando-se que não é admissível que os postos de trabalho tenham permissões de extração ou reprodução de imagens, função que só deve ser possível em máquinas dedicadas.

3.2.4. Em relação à manutenção do sistema de videovigilância, porque ela está diretamente relacionada com a segurança da informação e a aptidão do sistema para cumprir a finalidade, importa sublinhar que essa obrigação recai sobre o responsável pelo tratamento de dados, independentemente de quem seja o proprietário das câmaras de vídeo e demais equipamentos que componham o sistema.

Estabelecendo a Lei n.º 1/2005, no n.º 2 do artigo 2.º, que o responsável pelo tratamento dos dados *é a força de segurança com jurisdição na área de captação ou o serviço de segurança requerente*, eventual subcontratação em empresa para assegurar a manutenção ou substituição dos equipamentos tem de ser formalizada, contratualmente, com a PSP. Não está afastada a hipótese de a PSP subcontratar a Câmara Municipal da Amadora, podendo esta subsubcontratar empresas, nos termos regulados no artigo 23.º da Lei n.º 59/2019, de 8 de agosto.

III. CONCLUSÃO

Não cabendo na competência que lhe está legalmente atribuída pronunciar-se sobre os concretos fundamentos do alargamento do sistema de videovigilância na cidade da Amadora, a CNPD, com os argumentos acima expostos:

1. Destaca que:
    a. As incivilidades ou outras condutas que, ainda que ilícitas, se apresentam em tensão com a mera ordenação social não justificam a legitimação da restrição de direitos, liberdades e garantias por via deste tipo de sistemas de informação;
    b. Do mesmo modo, a pretensão de utilizar um sistema de videovigilância (quanto às câmaras n.ºs 62 a 139) com o âmbito e extensão do aqui considerado, para *monitorizar a circulação de pessoas e viaturas* vai muito para além da finalidade

legalmente definida invocada neste procedimento, não tendo, na verdade, qualquer enquadramento legal e constitucional;

E, assim, entende que o tratamento de dados pessoais realizado com a utilização do sistema de videovigilância na cidade da Amadora deve ater-se à finalidade de proteção da segurança de pessoas e bens em relação a condutas criminalizadas e de prevenção criminal, de acordo com a lei e a Constituição portuguesa.

2. Ainda assim, mesmo para esta finalidade, a utilização de Inteligência Artificial (máxime, de soluções de *soft recognition* e *Machine Learning*) nos sistemas de videovigilância carece de um específico enquadramento em termos de pressupostos e condições ou limites da sua aplicação, o qual, no caso, não existe, não tendo sequer sido objeto de apreciação na avaliação de impacto sobre a proteção de dados apresentada; nestes termos, a CNPD entende não ser admissível a sua utilização.

3. Também a utilização de um sistema biométrico de reconhecimento facial na cidade da Amadora carece de específico fundamento legal, estando, por isso, manifestamente vedada.

4. A CNPD recomenda ainda que sejam corrigidos os aspetos do tratamento de dados pessoais realizado com a utilização do sistema de videovigilância explanados no ponto 3.2.

Lisboa, 17 de julho de 2020

Filipa Calvão (Presidente, que relatou)